UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,975	04/02/2004	Narasimhan Sundararajan	MS#305305.01 (5228)	1693

38779 7590 06/28/2007

SENNIGER POWERS (MSFT)
ONE METROPOLITAN SQUARE, 16TH FLOOR
ST. LOUIS, MO 63102

EXAMINER
SAN JUAN, MARTINJERIKO P

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
06/28/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@senniger.com

Office Action Summary	**Application No.** 10/816,975	**Applicant(s)** SUNDARARAJAN, NARASIMHAN	
	Examiner Martin Jeriko P. San Juan	**Art Unit** 2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 April 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 April 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *April 2, 2004*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) ☒ Other: *See Continuation Sheet*.

Continuation of Attachment(s) 6). Other: 2nd IDS filed on October 11, 2005.

DETAILED ACTION

This is a response to the following case application:

Non-provisional Application: 10/816975 filed on April 2, 2004.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claim 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Wray [US Pub 2001/0010076 A1].

a. Based on claim 1, Wray teaches a method for authenticating the sender of a digital object, comprising: generating a first unique identifier (UID) [Alice is generating g^a where a is a random number. Par 0056-0057 and Par 0068]; transmitting to a previously known address, via an electronic mail protocol, a first message comprising the first UID [Alice is transmitting g^a. Fig 5]; receiving, via the electronic mail protocol, a second message comprising a second UID and a copy of the first UID [Alice is receiving g^b and SIG_b. SIG_b contains a signed copy of g^a, Par 0061]; and transmitting to the previously known address, via the electronic mail protocol, a third message comprising a copy of the second UID

[Alice is transmitting SIG_a. SIG_a contains a signed copy of g^b. Par 0061]; wherein at least one of the messages transmitted to the previously known address further comprises the digital object [Certificate attributes, JUST, that are linked to public keys are contained in the 2nd and 3rd messages. Fig 5].

b. With regard to claim 2, Wray teaches the method of claim 1 wherein the first message further comprises the digital object. [The digital object here is the Definition of G being sent to establish the secret key of the session. Fig 5.]

c. With regard to claim 3, Wray teaches the method of claim 1 wherein the third message further comprises the digital object. [The digital object here is a Certificate attribute, JUST, linked to the public key of Alice. Fig 5.]

d. With regard to dependent claim 4, Wray teaches the method of claim 1 wherein the digital object is a public key for a cryptographic system. [Public keys are inherent in Certificate attributes being exchanged. Par 0073, Par 0032.]

e. With regard to claim 5, Wray teaches the method of claim 4 wherein the second message further comprises a second public key for a cryptographic system. [A certificate attribute, $JUST_b$, has also been exchanged on the second message which is linked to Bob's public key.]

f. With regard to claim 6, Wray teaches the method of claim 1 wherein the electronic mail protocol comprises a mail server operating the Simple Mail Transport Protocol (SMTP). [Par 0006. SMTP is a protocol inherent in e-mails. SMTP is a standard protocol for e-mail messaging.]

g. With regard to claim 7, Wray teaches the method of claim 1 wherein at least a portion of the electronic mail protocol operates securely using the Transport Layer Security (TLS) protocol. [Par 0159. (SSL protocol has recently been standardized as the TLS. Par 0002)]

h. With regard to dependent claim 8, Wray teaches the method of claim 1 wherein the first UID contains at least 128 bits. [It is inherent that the first UID be at least 128 bits to meet ANSI X9.42 standard draft for Diffie Hellman key exchange protocol.]

i. Based on claim 9, Wray teaches the method for authenticating the sender of a digital object, comprising: receiving, via an electronic mail protocol, a first message comprising a first unique identifier (UID) [Bob receiving g^a. Fig 5]; generating a second UID [Bob generating g^b where b is a random number. Par 0056]; transmitting to a previously known address, via the electronic mail protocol, a second message comprising the second UID and a copy of the first UID [Bob transmits g^b and SIG_b. SIG_b contains a signed copy of g^a. Par 0061]; and receiving, via the electronic mail protocol, a third message comprising a copy of the second UID [Bob receiving SIG_a. SIG_a contains a signed copy of g^b. Par 0061]; wherein at least one of the messages received further comprises the digital object.

j. With regard to claim 10, Wray teaches the method of claim 9 wherein the first message further comprises the digital object. [The digital object here is the Definition of G being sent to establish the secret key of the session. Fig 5.]

k. With regard to claim 11, Wray teaches the method of claim 9 wherein the third message further comprises the digital object. [The digital object is a Certificate attribute, $JUST_A$ linked to a public key of the sender. Fig 5.]

l. With regard to claim 12, Wray teaches the method of claim 9 wherein the digital object is a public key for a cryptographic system. [Public keys are inherent in Certificate attributes being exchanged. (Par 0032)]

m. With regard to claim 13, Wray teaches the method of claim 12 wherein the second electronic mail message further comprises a second public key for a cryptographic system. [A certificate attribute, $JUST_b$ has been exchanged on the second message which is linked to a public key.]

n. With regard to claim 14, Wray teaches the method of claim 9 wherein the electronic mail protocol comprises a mail server operating the Simple Mail Transport Protocol (SMTP). [Par 0006. SMTP is a protocol inherent in e-mails. SMTP is a standard protocol for e-mail messaging.]

o. With regard to claim 15, Wray teaches the method of claim 9 wherein at least a portion of the electronic mail protocol operates securely using the Transport Layer Security (TLS) protocol. [Par 0159. (SSL protocol has recently been standardized as the TLS. Par 0002)]

a. With regard to dependent claim 16, Wray teaches the method of claim 9 wherein the first UID contains at least 128 bits. [It is inherent that the first UID be at least 128 bits to meet ANSI X9.42 standard draft for Diffie Hellman key exchange protocol.]

p. With regard to claims 17, and 20, these claims are rejected as applied to the like elements of claim 1.

q. With regard to claims 18, and 19, these claims are rejected as applied to the like elements of claims 4 and 5 respectively.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: [Rescorla, E. "RFC 2631-Diffie-Hellman Key Agreement Method." June 1999, RTFM Inc.]

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Jeriko P. San Juan whose telephone number is 571-272-7875. The examiner can normally be reached on M-F 7:30a - 5:00p EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJSJ

JOSEPH DEL SOLE
SUPERVISORY PATENT EXAMINER
6/21/07